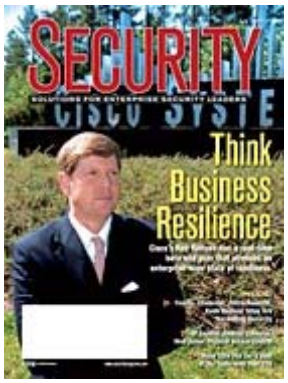
‘Beta Site’ World: Building a Resilient Business

by Gino Zucca
Rob Rolfsen

Posted: July 1, 2007



At Cisco, crisis drills are conducted on a regular basis. During the drills, wild cards are thrown out at people, who test their relationships and abilities, said Rob Rolfsen.

Now-a-days, corporations face a variety of crises that cause more damage more quickly than ever before.

Bigger storms, broader scandals, larger data thefts and more credible terrorist threats across the globe have the capacity to take down an unprepared business in a short time. Despite this, many corporations lack a comprehensive program to ensure the resilience of their business in the face of a catastrophic event. Not only does this put them at greater risk in the event of a crisis, it deprives them of the added value of a holistic business resiliency program.

Business resiliency is a relatively new term that represents an enterprise-wide state of readiness – an ability to quickly identify, react to and recover from business interruptions of any kind. It incorporates and more tightly aligns the more familiar functions of emergency response, business continuity, crisis management and disaster recovery.

Even when they’re managed separately, these functions should be intuitively interdependent. But by unifying them under a resiliency program, a corporation can maximize the use of available resources, create a greater awareness of risk and continuity issues and ensure that each involved group understands its responsibilities and those of its counterparts.

TERMINOLOGY OF RESILIENCY

Confusion between familiar terms like emergency response, business continuity, and crisis management often makes it difficult for executives to understand what programs they actually have in place. Before exploring how a resiliency program can tighten the bonds between its component functions, it’s important to nail down some definitions.

EMERGENCY RESPONSE

Emergency response provides the initial, on-site assessment of an incident. What is the situation, how are we impacted, and does this incident warrant further mitigative or responsive action on the part of the business? This function includes triage -- emergency medical teams and first response.

CRISIS MANAGEMENT

Crisis management is the process by which a business deals with an event that has been deemed significant. A situation has developed; now how do we react? Crisis management teams respond based upon a pre-determined plan of action that is appropriate to the event. They communicate and coordinate the corporate response across all business units to assess and re-assess impacted areas of the business and determine appropriate responses. This function includes everything from public relations management to evacuation and physical infrastructure analysis.

BUSINESS CONTINUITY

Business continuity is the ability of the business to continue operations during and after a crisis situation. This generally involves preparing and implementing manual workarounds to enable the business to respond to an interruption based upon previously determined and agreed-upon recovery time objectives. Business continuity often focuses on IT responsibilities, such as data backups and off-site storage. Many organizations call this function “disaster recovery.”

ENTERPRISE RISK MANAGEMENT

ERM is the discipline of holistically understanding and considering risk across all business units and locations in the enterprise. Security risks are not the only risks considered under an ERM model. In ERM, risks include everything from currency fluctuation, to geopolitical risks, to business model concerns, to basic security risks. The goal is to help the business make educated decisions on how to manage risk, both to better protect the enterprise and to identify opportunities for growth and profit.

The Business Resiliency umbrella covers emergencies, crisis, recovery and other business and security issues. ***Chart provided by the Security Executive Council.***

PIECING IT TOGETHER

A business resiliency program sets up a framework for all these elements of incident response that is developed and enforced at all levels of an organization. The result is a graduated, orchestrated incident response whose components share the goal of protecting employees and customers while maximizing shareholder value.

Escalation is built into the business resiliency model. The first group to be contacted in the event of an incident is the local emergency response team. The ERT assesses the situation and determines, based on criteria set by the business resiliency plan, whether the incident warrants alert or activation of the next level of response: crisis management. If it does, a local or regional crisis management team is called in to administer the launch of the crisis management program. All departments, including HR, travel, facilities, IT, public relations and sales, may be represented on this team.

If regional crisis management determines that the incident will affect the corporation as a whole—again judging the incident against pre-set criteria—it will alert the next level, which is corporate crisis management. Business continuity exercises often begin at this level. The corporate crisis management team deals with issues such as maintaining the corporate image, aggregating information from the local CMTs and communicating updates to individual locations and departments.

Technology plays a crucial role here. A technologically advanced emergency operations center with powerful IP capabilities can greatly assist the corporate and regional crisis management teams in communicating with one another and with customers and employees, and it can also help the business track the impact of the incident across locations.

All corporate entities are held accountable for business resiliency, with crisis management and business continuity built into every department's operational plans.

Enterprise risk management and business resiliency partner closely before, during and after a disruptive event. Business resiliency, like ERM, deals with more than security — it aims to pull the business through any interruption, whether physical, economic, or otherwise. Only with an enterprise risk program in place can the company ensure that the business resiliency plan focuses on the top risks and considers all the security and non-security risks that might impact the business.

WHAT IS THE VALUE?

Rob Rolfsen, a member of the Security Executive Council and director in enterprise risk management for Cisco Systems, defines business resiliency as a relatively new term that represents an enterprise-wide state of readiness.

Given all the crises we've seen in the United States and around the world over the past 10 years, it's surprising to discover that some organizations might not see the value in a business resiliency program. The Council on Competitiveness, a group of corporate CEOs, university presidents and labor leaders committed to enhanced U.S. competition in the global economy, has released a number of reports that show that while the payoff of a resiliency program is sometimes difficult to quantify, it is definitely there.

Effective business resilience reduces loss due to business interruption because the corporation has a practiced plan to work through and recover from the crisis as quickly as possible. The technology used for emergency operations and situational awareness may, where appropriate, find additional uses within the corporation, allowing it to become a profit center instead of a static cost. These include technologies like online collaborative tools, unified communications and mobility solutions that enhance emergency response and day-to-day productivity of the workforce.

Just days after Hurricane Katrina in 2005, Wal-Mart Stores Inc. was able to reopen 70 of its affected locations and begin routing critical supplies to those stores to help the recovery effort. Less than one month later,

CNN/Money noted that the company's quick reaction and philanthropic effort both silenced its many critics and forever endeared itself to the many consumers impacted by the storm. Examples like this are helping many companies to recognize that when they showcase their ability to bounce back from interruptions, they are strengthening their brand image and value, creating a competitive advantage.

SIDEBAR: The Upside of Security

From Debra van Opstal — When many CEOs hear the word security, they tend to think sunk cost, not strategic opportunity. For these companies, security tends to be reactive, de-centralized and ad hoc. The Council on Competitiveness has conducted studies on this topic across five industries — chemical, electric power and natural gas, financial services, oil and pharmaceutical. Two trends emerged during our research.

First, in all of the sectors, the risk landscape is changing – and not for the better. The globalization of business in a world of technological complexity and interdependencies has vastly complicated the risk management picture. This increase in risk has also created opportunities for security that go beyond just loss avoidance.

Second, the leader companies are transforming the way they think about – and manage – security and risk. Security is "baked into" every process and investment decision, not relegated to a back-office function that is bolted onto the business.

Integrating security into business processes yields some immediate bottom-line benefits: insight into workflow efficiencies, reduced losses from fraud or waste, and savings on insurance premiums.

At Georgetown University, for example, investments in housing infrastructure – the critical component of the tuition revenue stream – led to reductions in insurance premiums. The savings were used to buy business interruption insurance, which resulted in a high bond rating and a lower cost of capital.

Some companies, such as Waste Management, are taking advantage of the technologies and capabilities developed for security to create whole new business lines. Waste Management has created a new centralized security center that not only streamlined costs across 2,000 sites but also has become one of the fastest-growing profit centers for the company.

For some companies, the added confidence for the brand, the shareholders, customers and employees have become an integral part of the benefits calculation. What CEOs and Boards should know is that companies make money by taking risks, but they lose money by failing to manage them effectively.

SIDEBAR: Tabletops for Program Development

At Cisco, crisis drills are conducted on a regular basis. In addition, the firm's done five tabletop exercises on avian flu, where they pull together the team and run through

various scenarios testing pandemic preparedness and emergency response. The drill may begin with a fictional report of new cases of H5N1 reported out of Asia. They throw in compounding events like reports of major company-sponsored events in the affected region, which have ended, sending a large number of employees back to their local offices, and there is now an infection discovered halfway around the world. Drills can go all the way up to a full-blown activation of the crisis management team.

During the drills, wild cards are thrown out at people, which test their relationships. They hand out cue cards, each of which deals with a specific issue, and leaders may intentionally give a card or two to the wrong person. If they understand the functions of everybody else at the table, they know to say, “Hey, this isn’t mine – I need to give this to HR.”

Discovered: The tabletop exercises are very effective not just in testing existing plans but also in developing new ones. If you don’t yet have a resiliency program, this will test your current ability to respond, and you will quickly find your most significant points of weakness. There also are numerous private-public crisis management projects throughout the U.S. in which a component is training exercises. Check out this month's News & Analysis section.

Gino Zucca
Gino Zucca is senior manager of enterprise risk management for Cisco Systems. For information about the Security Executive Council, visit www.csoexecutivecouncil.com/?sourceCode=secmag

Rob Rolfsen
Rob Rolfsen is a member of the Security Executive Council and director in enterprise risk management for Cisco Systems.